

Construction of LDGM lattices

Hassan Mehri* and Mohammad Reza Sadeghi

*Faculty of Mathematics and Computer Science,
Amirkabir University of Technology,
No.424, Hafez Avenue, Tehran 15875-4413, Iran,*

March 4, 2013

Abstract

Low density generator matrix (*LDGM*) codes have an acceptable performance under iterative decoding algorithms. This idea is used to construct a class of lattices with relatively good performance and low encoding and decoding complexity. To construct such lattices, Construction *D* is applied to a set of generator vectors of a class of *LDGM* codes. Bounds on the minimum distance and the coding gain of the corresponding lattices and a corollary for the cross sections and projections of these lattices are provided. The progressive edge growth (PEG) algorithm is used to construct a class of binary codes to generate the corresponding lattice. Simulation results confirm the acceptable performance of these class of lattices.

Index Term: Lattice, PEG algorithm, *LDGM* codes.

1 INTRODUCTION

The lattice version of the Gaussian channel coding problem for a given value of signal to noise ratio (SNR) is to find the n -dimensional lattice for which the error probability is minimized [3]. It is shown that, lattices can achieve the

*Corresponding Author. *E-mail Address:* hassanmehri.math@gmail.com

capacity of additive white Gaussian noise (AWGN) channel [4, 5]. This fact motivates the search for lattices with large coding gains. On the other hand in larger dimensions the encoding and decoding complexity also increase. There are several methods to construct lattice from linear codes [3]. Among them, Construction **D** and Construction **D'** can produce high coding gain lattices by using a collection of linear codes. The idea of Low density generator matrix codes were first provided by Garcia and Zhong [6]. In addition to low encoding and decoding complexity, these linear codes have relatively good performance. As a result, constructing lattices based on these codes can be a promising tool. Therefore we will propose a class of lattices with almost high coding gain and low encoding and decoding complexity. The paper begins in the next section with a brief discussion about lattice. Section three introduces the Construction **D** lattices. Systematic low density generator matrix lattices discussed in the forth section. The final section is dedicated to the paper's conclusions.

2 BACKGROUND

Low density generator matrix (*LDGM*) codes are linear codes which have sparse generator matrix [6]. Let \mathbb{R}^m be the m -dimensional real vector space with the standard product $\langle \cdot, \cdot \rangle$ and Euclidean norm $\| \mathbf{x} \| = \langle \mathbf{x}, \mathbf{x} \rangle^{1/2}$. An n dimensional lattice in \mathbb{R}^m is defined as the set of all linear combinations of a given basis of n linearly independent vectors in \mathbb{R}^m with integer coefficients [3]. Any subgroup of a lattice Λ is called sublattice of Λ and a lattice is called *orthogonal* if it has a basis with mutually orthogonal vectors. The set Λ^* of all vectors in the real span of Λ ($span(\Lambda)$), whose the standard inner product with all elements of Λ has an integer value, is an n -dimensional lattice called the *dual* of Λ . Lattices constructed by Construction **D** have a square generator matrix thus if \mathbf{B} is a generator matrix for Λ , then $\mathbf{B}^* = \mathbf{B}^{-1}$ is a generator matrix for Λ^* (parity-check matrix of Λ). Every lattice point is therefore of the form $\mathbf{v} = \mathbf{B}\mathbf{x}$ where \mathbf{x} is an n -dimensional vector of integers. The Voronoi cell of a lattice point is defined as the set of all points in \mathbb{R}^m that are closer to this lattice point than to other lattice point. The Voronoi cells of all lattice points are congruent and for Lattices constructed by Construction **D** the volume of the Voronoi cell is equal to volume of Λ [3]. The coding

gain of lattice Λ is defined by

$$\gamma(\Lambda) := \frac{d_{min}^2(\Lambda)}{\det(\Lambda)^{2/n}}, \quad (1)$$

where $d_{min}(\Lambda)$ and $\det(\Lambda)$ refer to minimum distance and volume of Λ , respectively [3]. Assume an n -dimensional lattice Λ with an n -dimensional orthogonal sublattice Λ' which has a set of basis vectors along the orthogonal subspace $S = \{W_i\}_{i=1}^n$. By the definition of the projection onto the vector space W_i as P_{W_i} and the cross section Λ_{W_i} as $\Lambda_{W_i} = \Lambda \cap W_i$. Now, the *label groups* G_i is defined as $G_i = P_{W_i}/\Lambda_{W_i}$, which is used to label the cosets of Λ' in Λ . Let $|G_i| = g_i$ and \mathbf{v}_i be the generator vector of Λ_{W_i} , i.e., $\Lambda_{W_i} = \mathbb{Z}\mathbf{v}_i$. Each element of G_i can be rewritten in the form of $\Lambda_{W_i} + j \det(P_{W_i})\mathbf{v}_i/|\mathbf{v}_i|(j = 1, \dots, g_i - 1)$. Then the map

$$\Lambda_{W_i} + j \det(P_{W_i}) \frac{\mathbf{v}_i}{|\mathbf{v}_i|} \longrightarrow j \quad (2)$$

is an isomorphism between G_i and \mathbb{Z}_{g_i} , thus every element of the label group G_i can be written as $(\mathbb{Z} + a_j)\mathbf{v}_i$, where $a_j = j \det(P_{W_i})/\det(\Lambda_{W_i})$ [1].

3 CONSTRUCTION \mathbf{D} LATTICES

Between other constructions of lattices from linear codes, Construction \mathbf{D} seems to be one of the best choices for constructing lattices from *LDGM* codes [2]. This construction can produce lattices with high coding gains and it deal with generator sets of codes.

Let $\alpha = 1$ or $\alpha = 2$ and $C_0 \supseteq C_1 \supseteq \dots C_a$ be a family of binary linear codes, where the code C_l has parameters $[n, k_l, d_{min}^{(l)}]$ with $d_{min}^{(l)} \geq 4^l/\alpha$, for $l = 1, \dots, a$ and C_0 is the trivial code \mathbb{F}_2^n . Choose a basis $\{\mathbf{c}_1, \dots, \mathbf{c}_n\}$ for \mathbb{F}_2^n such that $C_l = \langle \mathbf{c}_1, \dots, \mathbf{c}_{k_l} \rangle$. For any element $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{F}_2^n$ consider

$$\frac{\mathbf{x}}{2^{l-1}} = \left(\frac{x_1}{2^{l-1}}, \dots, \frac{x_n}{2^{l-1}} \right)$$

as a vector in \mathbb{R}^n . Then $\Lambda \subseteq \mathbb{R}^n$ consists of all vectors of the form

$$\mathbf{z} + \sum_{l=1}^a \sum_{j=1}^{k_l} \frac{\alpha_j^{(l)}}{2^{l-1}} \mathbf{c}_j, \quad (3)$$

where $\mathbf{z} \in (2\mathbb{Z})^n$ and $\alpha_j^{(l)} = 0, 1$.

Theorem 3.1: The set Λ is a lattice, with minimum distance at least $4/\alpha$, determinant

$$\det(\Lambda) = 2^{n - \sum_{l=1}^a k_l}, \quad (4)$$

and coding gain of Λ is

$$\gamma(\Lambda) \geq \alpha^{-1} 4^{\sum_{l=1}^a \frac{k_l}{n}}. \quad (5)$$

An integral basis for Λ is given by the vectors

$$\frac{1}{2^{l-1}} \mathbf{c}_j \quad \text{for } l = 1, \dots, a \quad \text{and} \quad j = k_{l+1} + 1, \dots, k_l,$$

plus $n - k_1$ vectors of the form $(0, \dots, 0, 2, 0, \dots, 0)$.

The proof is given in the appendix.

Corollary 3.1: Let \mathbf{B} be the generator matrix of the lattice constructed using Construction **D**. For any $1 \leq j \leq n$, and for $k_{l+1} + 1 \leq s_j \leq k_l$, such that $k_{a+1} = 0$. Let s_j be the smallest number such that $[\mathbf{B}_{s_j, j}] \neq 0$ and Λ_{w_j} be the cross section of Λ in the coordinate system $W_j = \langle e_j \rangle$. Then $\Lambda_{w_j} = 2\mathbb{Z}$ and $P_{w_j}(\Lambda) = \mathbb{Z}/2^{l-1}$.

The proof is given in the appendix.

Example 3.1: Let $a = 1, \alpha = 2$ and C_0, C_1 are two linear codes whose C_0 be the trivial code \mathbb{F}_2^7 and C_1 be the $(7, 4)$ linear code “Hamming code” thus the lattice constructed using Construction **D** has the following Generator and parity-check matrices:

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}, \quad \mathbf{B}^* = \begin{pmatrix} 1 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} & 0 \\ 0 & 1 & 0 & 0 & 0 & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 1 & 0 & -\frac{1}{2} & -\frac{1}{2} & -\frac{1}{2} \\ 0 & 0 & 0 & 1 & -\frac{1}{2} & 0 & -\frac{1}{2} \\ 0 & 0 & 0 & 0 & \frac{1}{2} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{1}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & \frac{1}{2} \end{pmatrix}$$

Corollary 3.1, implies that $s_1 = 1$, $s_2 = 2$, $s_3 = 3$, $s_4 = 4$, $s_5 = 1$, $s_6 =$

1, $s_7 = 2$. Therefore $\Lambda_{w_j} = 2\mathbb{Z}$, $P_{w_j}(\Lambda) = \mathbb{Z}$ and $|G_j| = 2$ ($j = 1, \dots, 7$).

The following theorem, which generalizes Construction **D** to any collection of linear codes without condition $d_{min}^{(l)} \geq \frac{4^l}{\alpha}$, is proved. This theorem shows the relation between the performance of the lattice and the performance of its linear codes.

Theorem 3.2: Let $C_0 \supseteq C_1 \supseteq \dots \supseteq C_a$ be a family of linear codes with $C_l = [n, K_l, d_{min}^{(l)}]$ and let $\{\mathbf{c}_1, \dots, \mathbf{c}_n\}$ be linear independent vectors in \mathbb{F}_2^n such that

$$C_l = \langle \mathbf{c}_1, \dots, \mathbf{c}_{K_l} \rangle, \quad l = 1, \dots, a.$$

Also let Λ be the corresponding lattice given by Construction **D**. Then we have

$$\frac{1}{\alpha} \min\{d_{min}^{(1)}, 4^{-1}d_{min}^{(2)}, \dots, 4^{1-a}d_{min}^{(a)}, 4\} \leq d_{min}^2(\Lambda) \quad (6)$$

The proof is given in the appendix.

Corollary 3.2: The coding gain of the lattice constructed using Construction **D** is

$$\frac{\frac{1}{\alpha} \min\{d_{min}^{(1)}, 4^{-1}d_{min}^{(2)}, \dots, 4^{1-a}d_{min}^{(a)}, 4\}}{4^{1 - \frac{\sum_{l=1}^a K_l}{n}}} \leq \gamma(\Lambda). \quad (7)$$

and if $d_{min}^{(l)} \geq 4^l$, $l = 1, \dots, a$, then

$$\alpha^{-1} 4^{\frac{\sum_{l=1}^a K_l}{n}} = \gamma(\Lambda). \quad (8)$$

The proof is given in the appendix.

4 SYSTEMATIC *LDGM* LATTICES

In order to have a low iterative decoding complexity, we need to have a low density Tanner graph representation for the lattice [1]. To achieve this goal the new class of lattices “*systematic low density generator matrix (SLDGM) lattices*”, from systematically *LDGM* codes is constructed. It is known that

when the girth (the length of the shortest cycle in the Tanner graph) of code's increases, then the minimum distance of the code also increases [10]. The progressive edge growth (PEG) algorithm is an efficient method for constructing a Tanner graph having a large girth by progressively establishing edges between symbol and check nodes in an edge-by-edge manner [9]. For *SLDGM* lattices Corollary 3.1 implies that $g_i = 2^l$, for some $l \in \{1, \dots, a\}$. If $\alpha = 1$ and $a = 1$, then one-level *SLDGM* lattices are obtained, we denoted by $SLDGM_n^1$ and if $a = 2$ then two-level *SLDGM* lattices derived which are denoted by $SLDGM_n^2$.

The Generalized Min-Sum Algorithm For Lattices Constructed Using Construction **D** is used to decode *SLDGM* lattices [7]. The upper bound of decoding complexity per iteration is:

$$N_{dec} \leq n(g \cdot d_s^{max}(d_s^{max} - 1) + g^{d_{ch}^{max}} \cdot d_{ch}^{max}(d_{ch}^{max} - 1) + g - 1) \quad (9)$$

where d_s^{max} and d_{ch}^{max} are the maximum degree of symbol-nodes and check-nodes in the Tanner graph of the lattice respectively and $g_i \leq g$ ($i = 1, \dots, n$).

In the following tables the performance of *SLDGM*_{*n*} lattices compared with *LDPC* lattices (*L_n*) [8]. In these tables $N_D = N_{dec} \times (\text{average number of iteration})$ and M_I denote the decoding complexity and maximum number of iteration, respectively. $P_e^* = (2/n)P_e$ denotes the normalized error probability[11].

Table.1

| SNR_{db} | N_D | M_I | P_e | P_e^* |
|------------|-------------------------|-------|------------------------|------------------------|
| 1 | $\leq 3.87 \times 10^5$ | 7 | 7.98×10^{-1} | 6.23×10^{-3} |
| 2 | $\leq 3.03 \times 10^5$ | 6 | 2.65×10^{-1} | 2.031×10^{-3} |
| 3 | $\leq 2.70 \times 10^5$ | 4 | 3.71×10^{-2} | 2.889×10^{-4} |
| 4 | $\leq 2.45 \times 10^5$ | 4 | 7.967×10^{-3} | 6.22×10^{-5} |
| 5 | $\leq 2.14 \times 10^5$ | 3 | 4.00×10^{-4} | 3.125×10^{-6} |
| 6 | $\leq 1.5 \times 10^5$ | 2 | 2.003×10^{-5} | 1.56×10^{-7} |

performance of *SLDGM*₂₅₆¹

Table.2

| SNR_{db} | N_D | M_I | P_e | P_e^* |
|------------|--------------------|-------|------------------------|------------------------|
| 1 | 1.9×10^6 | 35 | 5.807×10^{-1} | 4.536×10^{-3} |
| 2 | 9.5×10^5 | 36 | 1.209×10^{-1} | 9.453×10^{-4} |
| 3 | 4.66×10^5 | 35 | 1.759×10^{-2} | 1.375×10^{-4} |
| 4 | 2.74×10^5 | 35 | 2.396×10^{-3} | 1.872×10^{-5} |
| 5 | 2.33×10^5 | 32 | 2.46×10^{-4} | 1.92×10^{-6} |
| 6 | 2.25×10^5 | 28 | 1.20×10^{-5} | 9.375×10^{-8} |

performance of L_{256}^1

The performance of one-level type of these lattices show that for decoding *SLDGM* lattices we didn't need large number of iteration as done as for *LDPC* lattices. one-level *SLDGM* lattices have almost the same performance like one-level *LDPC* lattices. The performance of two-level type of these lattices at the same dimension is proposed as follows:

Table.3

| SNR_{db} | N_D | M_I | P_e | P_e^* |
|------------|-------------------------|-------|-----------------------|-----------------------|
| 1 | $\leq 2.70 \times 10^5$ | 13 | 7.10×10^{-1} | 5.54×10^{-3} |
| 2 | $\leq 2.38 \times 10^5$ | 7 | 3.23×10^{-1} | 2.52×10^{-3} |
| 3 | $\leq 1.87 \times 10^5$ | 6 | 8.02×10^{-2} | 6.95×10^{-4} |
| 4 | $\leq 1.46 \times 10^5$ | 4 | 1.00×10^{-2} | 7.81×10^{-5} |

performance of $SLDGM_{256}^2$

Table.4

| SNR_{db} | N_D | M_I | P_e | P_e^* |
|------------|--------------------|-------|-----------------------|------------------------|
| 1 | 2.76×10^6 | 23 | 9.51×10^{-1} | 7.439×10^{-3} |
| 2 | 2.11×10^6 | 21 | 3.41×10^{-1} | 2.666×10^{-3} |
| 3 | 1.20×10^6 | 23 | 7.35×10^{-3} | 5.754×10^{-5} |

performance of L_{256}^2

The upper bound of decoding complexity for *SLDGM* lattices is lower than decoding complexity for *LDPC* lattices. As mentioned before maximum number of iteration for decoding *SLDGM* lattices is lower than it for *LDPC* lattices. Two-level *SLDGM* lattices have relatively the same performance like two-level *LDPC* lattices.

These results show that *SLDGM* lattices have almost good performance. The *LDPC* lattices encoder has to calculate the generator matrix. Not that unlike \mathbf{B}^* , $\mathbf{B} = (\mathbf{B}^*)^{-1}$ is not sparse matrix, in general, so the calculation requires nonlinear computational complexity. This not a desirable property because the decoder's computational complexity is linear [8]. A possible solution is to produce *LDGM* lattices which have linearly encoding and decoding complexities.

5 CONCLUSION

With a slight modification in the structure of Construction **D**, A new class of lattices in terms of their generator matrix is proposed. Theorem 3.2 provides

lower bound on minimum distance of the lattice in terms of the minimum distance of its underlying codes. Corollary 3.2 shows the relation between the coding gain of the lattice and its underlying codes parameters. It is shown that cross sections and projections of this class of lattices can be derived properly. In addition to low encoding and decoding complexities, these class of lattices have an acceptable performance under iterative decoding algorithm. The performance of the *LDGM* lattices depends on the performance of their underlying *LDGM* codes. It would be interesting to construct other class of *LDGM* lattices. Such constructions would improve, or provide us with different performance compared to the class of *LDGM* lattices presented here.

6 APPENDIX

Theorem 3.1: The proof is given in [2].

Corollary 3.1: By the definition of cross section and projection of a lattice, the result is a direct consequence of *Theorem 3.1*

Theorem 3.2: We have $\frac{1}{\alpha} \leq d_{min}^{(0)}$, because $C_0 = \mathbb{F}_2^n$. Consider $\mathbf{x} \neq 0 \in \Lambda$, without loss of generality choose $k \geq 0$ such that $2^k \mathbf{x} \in \mathbb{Z}^n$ and $2^{k-1} \mathbf{x} \notin \mathbb{Z}^n$. Let $k \leq a - 1$, Eq(2) yields there would be $l \in \{1, \dots, a\}$ such that $\alpha_j^{(l)} \neq 0$ thus we could find $1 \leq j \leq k_l$ such that $\mathbf{c}_j \neq 0$ where $\mathbf{c}_j = (c_{j_1}, \dots, c_{j_n})$. Then there would be $j_1 \leq j_m \leq j_n$ which $c_{j_m} = 1$. Since $\mathbf{c}_j \in C_{K_l}$ as a result of Euclidean norm $\|\mathbf{c}_j\|^2 \geq \frac{d_{min}^{(l)}}{\alpha}$. It follows that

$$\left(\frac{1}{2^{l-1}}\right)^2 \|\mathbf{c}_j\|^2 \geq \frac{d_{min}^{(l)}}{\alpha} 4^{1-l},$$

Hence

$$\|\mathbf{x}\|^2 \geq \frac{d_{min}^{(l)}}{\alpha} 4^{1-l}.$$

Let $k \geq a$ then $\|\mathbf{x}\|^2 \geq \frac{4}{\alpha}$.

Corollary 3.2: The proof is a direct consequence of the *Theorem 3.2* and the definition of coding gain of the lattice.

References

- [1] A.H. Banihashemi, F.R. Kschinschang, “Tanner graphs for group codes and lattices: construction and complexity”, *IEEE Trans. Inf. Theory*, vol. 47, pp. 824–882, 2001.
- [2] E.S. Barnes, N.J.A. Sloane, “New lattice packings of spheres”, *Can.J.math*, vol. 35, pp. 117-130, 1983.
- [3] J.H. Conway, N.J.A. Sloane, Sphere Packing, Lattices and Groups (3rd ed.), Springer-Verlag, New York, 1999.
- [4] G.D. Forney, Jr., M.D. Trott, S.Y. Chung, “Sphere-Bound-Achieving coset codes and multilevel coset codes”, *IEEE Trans. Inf. Theory*, vol. 46, pp. 820-850, 2000.
- [5] G.D. Forney, Jr., “Approaching the capacity of the AWGN channel with coset codes and multilevel coset codes”, *ISIT*, 1997.
- [6] J. Garcia-Frias, W. Zhong, “Approaching Shannon performance by iterative decoding of linear codes with low-density generator matrix”, *IEEE Commun. Lett*, vol. 7, pp. 266-268, 2003.
- [7] H. Mehri, “Min-Sum algorithm for lattices constructed using construction **D**”, <http://arxiv.org/abs/1201.3982>.
- [8] M.R. Sadeghi, A. H. Banihashemi, D. Panario, “Low density parity check lattices: construction and decoding analysis”, *IEEE Trans. Inf. Theory*, vol. 52, pp. 4481-4495, 2006.
- [9] X-Y Hu, E. Eleftheriou and D. Arnold “Regular and irregular progressive edge-growth Tanner graphs”, *IEEE Trans. Inf. Theory*, vol. 51, pp. 386-398, 2005.
- [10] R.M. Tanner, “A recursive approach to low complexity codes”, *IEEE Trans. Inf. Theory*, vol. 27, pp. 533-547, 1981.
- [11] V. Tarokh, A. Vardy, “Universal bound on the performance of lattice codes”, *IEEE Trans. Inf. Theory*, vol. 45, pp. 670-681, 1999.